Vectra Detect Platform Software Update

The Vectra® X-series appliances, B-series appliances, S-series sensors, Cloud Brain, and Cloud Sensors, are scheduled to be updated to Vectra Detect for Network software release version 6.20

The Version 6.20 release introduces VMWare ESXi Brain support and O365 Detection Name Changes.

Vectra Detect platform enhancements and bug fixes are also included in this release.

Release Schedule

6.20 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on 7/13/2022
    - You can check if you have remote support enabled under Settings -> Services with Remote Support set to Enabled.
- **Customers Connected to Updater**: Customers who do not have remote support enabled but are connected to Updater will receive updates on 7/20/2022
    - You can check if you are connected to Updater under Settings->Services and see that Updater Destination shows as connected, while Remote Support shows disabled.
- **All Other Customers***: Will be able to download the update on 7/20/22.
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

VMWare ESXi Brain — Vectra Detect for Network

Vectra is pleased to introduce support for the VMWare ESXi Brain. This new platform supports the same features as the traditional hardware and cloud Brains, but is available in a virtual form factor supported on VMWare ESXi 6.5 and later. The VMWare Brain supports 2, 4, and 10Gbps configurations. For more information, please see the VMWare Brain Deployment Guide: https://support.vectra.ai/s/article/KB-VS-1592

Detection Name Change — Vectra Detect for O365

The detection name pre-fix “O365” used to denote attacker activity in Microsoft 365 will be changed to “M365” This change allows Vectra to better match Microsoft’s product naming.

Customers can continue to use the same naming convention when interacting with these detections in the API. All requests returned from the API will include the updated alert name. Detection events logged via syslog will appear with the new detection name.

Bug Fixes

CS-5690: Stream occasionally stops after upgrades

This addresses an issue when Kafka/SASL auth is configured with Stream, and will cause Stream to stop forwarding after upgrades. This has been addressed.

CS-5772: “Submit a Support Request” link no longer works

This addresses an issue where the workflow to submit a support ticket does direct the user to the proper location. This has been addressed.

CS-5657: Active Directory LDAP START_TLS does not work

When the Active Directory integration is configured with Start_TLS the LDAP bind does not work. This has been addressed.

CS-6037: Triage rule not being correctly applied

When a whitespace is included at the end of a detection detail, the Triage rule will not properly match. This has been addressed.

CS-6189: Stream cannot publish information after switching to 10Gbps Mgt interface on X29/M29

IIn 6.19, when using the 10Gbps management interface on the X29 with Stream enabled, Stream is unable to publish metadata information. This issue has been addressed.

SAASAPPS-1892: Brain returned as Sensor in Selective PCAP

In 6.19, Brain appliances were returned in the list of Sensors in Selective PCAP. Only Sensors/Mixed-mode appliances are supported to trigger PCAP's on. This fixes the issue where the Brain would be presented as a Sensor option to the user in Selective PCAP.

SAASAPPS-1873: Selective PCAP generated PCAPs with <#>.pcap rather than the name of the Capture.

In 6.19, when generating a PCAP, the filename of the PCAP would be the job ID number rather than the name of the job. To improve the user experience, Selective PCAP will name the PCAP by the job name rather than the ID.

SAASAPPS-1863: Deleting an Active capture was allowed in Selective PCAP

In 6.19, Detect would allow the user to attempt to delete an active capture, which is not a supported operation. The user must first stop the capture before they can delete it. This workflow condition has been addressed.

Known Issues

PCAP's collected in 6.19 will not be available after 6.20 upgrade

The naming convention of the PCAP file is changing from a ID number in 6.19 to a more user-friendly job name convention in 6.20. Captures that were taken in 6.19 prior to the 6.20 upgrade will not be available to download from the Brain after the upgrade. This is a one-time change. The recommended workaround is to download all 6.19 PCAP's from the Brain prior to upgrading to 6.20. This issue should not be present in future upgrades.

Appendix:

Will this upgrade perform a reboot of the Brain or Sensors?

This update will not perform any reboot of the Brain or Sensor appliances, nor is any user interaction required.